IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventor:	Yves AUDEBERT et al.	Art Unit 2132
Appln. No.:	09/844,246	Exr. B. Lanier
Filed:	April 30, 2001	Conf. No. 8917

For: METHOD AND SYSTEM FOR ESTABLISHING A REMOTE CONNECTION TO A PERSONAL SECURITY DEVICE

RESPONSE UNDER 37 CFR 1.111

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated November 1, 2007, the Applicants hereby petition for a three-month extension of time and respectfully request reconsideration and allowance of this application in light of the following remarks.

Claims 1-7, 9, 10, 15-17, 19-39, 41, and 42 stand rejected, under 35 USC §103(a), as being unpatentable over DiGiorgio et al. (US 6,385,729) in view of Elgamal et al. (US 5,657,390). Claims 18 and 40 stand rejected, under 35 USC §103(a), as being unpatentable over DiGiorgio in view of Elgamal and Brown et al. (US 5,455,863). Claims 1-7, 9, 10, and 15-42 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting. The Applicants respectfully traverse these rejections based on the points set forth below.

Claim 1 defines a system for establishing a communication pipe between a personal security device (PSD) and a remote computer system over a network having a local client serving as a host for the PSD. The local client connects the PSD to the network and (1) separates encapsulated APDUs from message packets that are received from the remote computer system and communicates the separated APDUs to the PSD, and (2) encapsulates APDUs received from the PSD into message packets that are communicated to the remote computer system.

As argued by Applicants in their Response dated March 19, 2007, and as cknowledged in section 2 of the Office Action dated April 20, 2007, DiGiorgio does not disclose the claimed features wherein: (1) a client routes APDUs received from a remote computer system to a PSD and (2) routes APDUs received from the PSD to the remote computer system. The present Office Action has resurrected a basis for rejecting claim 1 that the April 20, 2007, Office Action acknowledged to be incorrect; specifically, the present Office Action proposes that DiGiorgio's disclosure – "[w]hen a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services" – is identical to the claimed feature of separating encapsulated APDUs from message packets that are received from a remote computer system and communicating the separated APDUs to a PSD (see Office Action section 4, lines 9-14; Final Rejection dated July 19, 2006, section 6, lines 8-15; Office Action dated March 28, 2006 section 4, lines 8-15; and Final Rejection dated August 3, 2005, section 4, lines 8-15). In brief, the Office Action proposes that issuing a challenge from an ISP (i.e., DiGiorgio's remote server 16) to a token device (i.e., DiGiorgio's token 10) is identical to the claimed feature of separating encapsulated APDUs from message packets that are received from a remote computer system and communicating the separated APDUs to a PSD.

However, as argued by Applicants on pages 3 and 4 of their Response dated March 19, 2007, and as acknowledged in section 2 of the Office Action dated April 20, 2007, the proposed disclosure of issuing a challenge from an ISP to a token device does not expressly describe or inherently require that:

(A) the challenge issued by the ISP be in the form of APDUs or APDUs encapsulated in message packets;

(B) a client terminal interfacing the token device to the ISP separates the APDUs from the message packets received from the ISP; <u>or</u>

(C) the client terminal communicates the separated APDUs (i.e., the <u>identical</u> APDUs encapsulated by the ISP into message packets) to the token device. Thus, DiGiorgio fails to disclose the claimed feature of communicating APDUs from a remote computer system to a PSD and, more specifically, a client that separates encapsulated APDUs from message packets that are received from the remote computer system and communicates the separated APDUs to the PSD.

With regard to the claimed feature of encapsulating APDUs received from a PSD into message packets that are communicated to a remote computer system, the present Office Action has similarly resurrected an argument that the April 20, 2007, Office Action acknowledged to be incorrect; specifically, the present Office Action proposes that DiGiorgio's disclosure – "[o]nce the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B" – is identical to the claimed feature of a client that encapsulates APDUs received from a PSD into message packets that are communicated to a remote computer system (see Office Action section 4, lines 15-20; Final Rejection dated July 19, 2006, section 6, lines 15-20; Office Action dated March 28, 2006 section 4, lines 15-20; and Final Rejection dated August 3, 2005, section 4, lines 15-20). In brief, the Office Action proposes that issuing a response from a token device in the form of APDUs is identical to encapsulating APDUs received from a PSD into message packets that are communicated to a remote computer system.

However, as argued by Applicants on pages 4 and 5 of their Response dated March 19, 2007, and as acknowledged in section 2 of the Office Action dated April 20, 2007, the proposed disclosure of issuing a response in the form of APDUs from a token device 10 to an ISP 16 only requires that the token device issues APDUs. This proposed disclosure does not expressly describe or inherently require that:

(D) an intermediary client terminal (e.g., DiGiorgio's local computer 14) interfacing the token device 10 and ISP 16 encapsulates the APDUs received from the token device (i.e., the identical APDUs communicated by the token device) into message packets; or

(E) the client terminal 14 communicates the encapsulated APDUs to the ISP 16. Thus, DiGiorgio fails to disclose the claimed feature of a client that encapsulates APDUs received from a PSD into message packets that are communicated to a remote computer system.

The Office Action cites Elgamal for disclosing the feature of encrypting data communicated over a network between a local computer and a remote computer (see Office Action, sentence bridging pages 3 and 4). However, Elgamal does not disclose encrypting APDUs and does not supplement the teachings of DiGiorgio with respect to the claimed subject matter of: (1) separating encapsulated APDUs from message packets that are received from a remote computer system and communicating the separated APDUs to a PSD and (2) encapsulating APDUs received from a PSD interface into message packets that are communicated to a remote computer system.

In summary, neither DiGiorgio nor Elgamal disclose communicating APDUs between a PSD and a remote computer via a local computer hosting the PSD and a network interfacing the local computer and the remote computer. As a result, it necessarily follows that DiGiorgio and Elgamal cannot disclose encapsulating the APDUs for communication between the local computer and the remote computer. For elaborating upon these points, the Applicants draw the Office's attention to the remarks presented in Applicants': (1) Response dated March 19, 2007; (2) Response dated December 19, 2006; and (3) Response dated December 5, 2005.

In accordance with the above discussion, the Applicants respectfully submit that DiGiorgio and Elgamal, considered individually or in combination, do not render obvious the subject matter defined by claim 1. Independent claims 20, 29, and 42 similarly recite the above-described features distinguishing apparatus claim 1 from DiGiorgio and Elgamal, but with respect to methods. Therefore, the obviousness rejections applied to claims 18 and 40 are obviated and allowance of claims 1, 20, 29, and 42 and all claims dependent therefrom, is warranted.

The applied double patenting rejections are provisional. Applicants will address the double patenting rejections when the provisional status is removed.

To promote a better understanding of the differences between the claimed subject matter and the applied references, the Applicants provide the following additional remarks.

In support of its arguments that DiGiorgio discloses the claimed features of: (1) separating encapsulated APDUs from message packets that are received from a remote computer system and communicating the separated APDUs to a PSD, and (2) encapsulating APDUs received from the PSD into message packets that are communicated to the remote computer system, the Office Action cites DiGiorgio's column 2, lines 16-23, column 10, lines 24-35, and Fig. 8. In column 2, lines 16-23, DiGiorgio discloses that a user enters a PIN that is compared to a stored PIN in a secure token device and if a match occurs the user is granted access to a local computer system 14 (see DiGiorgio col. 10, lines 1-11). All such functions are carried out locally between the computer system 14 and the secure token device 10. There is no involvement of the ISP or remote server 16.

Fig. 8 illustrates a response APDU that is described in column 9, lines 35-43, and concerns only communications between the secure token device and the local computer system 14 using the Opencard API stored on the local computer system 14 and the Javacard API stored in the secure token device (see col. 7 line 19, through col. 9, line 43).

In fact, DiGiorgio's column 7, line 19, through column 9, line 43, makes it clear that communication using APDUs (whether command or response APDUs) takes place only between the secure token device and the local computer system 14 (see col. 5, lines 16-19). The local computer system 14 and the secure token device operate according to a Master-slave model and "the secure token device 10 always waits for a command APDU from the computer system by way of the reader 12" (see col. 9, lines 6-10). Communication using APDUs does not occur between the ISP/remote server 16 and the local computer system 14.

In fact, DiGiorgio discloses that the remote server 16 controlled by the ISP provides access to the internet and is linked to computer system 14 via a communications link 15 (see col. 5, lines 50-57). A web browser 72 is provided in primary storage 68 of the local computer system 14 to access the internet and processes HTML documents (see col. 7, lines 44-50). This would imply that communication occurs using a protocol such as Hyper Text Transfer Protocol, for example.

Consequently, communication between the secure token device 10 and the ISP/remote server 16 occurs in at least two separate steps: the ISP/remote server 16 communicates with the computer system 14 via a communications link 15; and the computer system 14 performs a data translation and communicates with the secure token device 10 using the Opencard standard, as stated at column 5, lines 26-37, and further explained below with respect to column 10, lines 24-35.

In column 10, lines 24-35, DiGiorgio discloses that a user accesses services of the ISP by double clicking an icon of the computer system. A two-way challenge response authentication is then initiated where the ISP issues a challenge to the secure token device. The secure token device responds and if the response is proper, the user is authenticated and the secure token device issues a challenge to the ISP.

However, with respect to communications between the secure token device and the ISP related to the challenge response authentication, the only detail specified is that "[t]he ISP applet 44 contains the appropriate intelligence for responding to such a challenge. The challenge may be issued by one of the applications 78 stored in the primary storage 68 of the computer system." Consequently, it can only be concluded from what is disclosed by DiGiorgio in column 5, lines

33-37, and column 7, line 19, through column 9, line 43, that the Opencard API 76 in association with another Java applet (see col. 7, lines 50-56) contained in the local computer system 14 interacts with the ISP applet 44 in the secure token device and passes APDU commands to the ISP applet 44 and the ISP applet 44 replies by passing APDU responses to the Java applet and the Opencard API 76, as is normal in the Opencard standard, in order to carry out the challenge response authentication.

Thus, it is a Java applet and an API running on the local computer system 14 that carries out the challenge function, to generate and send APDUs to the secure token device and to receive APDUs from the secure token device 10. The ISP does not generate APDUs, send APDUs, or send APDUs in an encapsulated message to the local computer system 14. Such a capability is only possible at the local computer system 14, as disclosed at column 7, line 19, through column 9, line 43. Such a capability using the Opencard standard and Javacard API is not described with relation to the ISP or remote sever 16. Consequently, in the absence of such capability being located at the ISP or remote sever 16, the generation of APDUs, the sending of APDUs, or the sending of APDUs in an encapsulated message to the local computer system 14 from the ISP or remote server 16 are all impossible. These capabilities and operations are disclosed nowhere in DiGiorgio or Elgamal with respect to the ISP or remote sever 16.

Moreover, the ISP or remote server 16 are not sent response APDUs from the local computer system 14 (such as that illustrated in Figure 8B, for example) as the ISP or remote server 16 disclosed in DiGiorgio does not have any technical capability to handle or process such a response APDU if it received a response APDU. Additionally, it is simply not disclosed in DiGiorgio that response APDUs are communicated from local computer system 14 to remote server 16/ISP. DiGiorgio solely discloses that response APDUs are communicated to the local computer system from the secure token device (see col. 7, line 19, through col. 9, line 43).

In fact, DiGiorgio is completely silent as to precisely how the challenge response authentication is carried out between the ISP and the secure token device and to how any communication between the ISP and the secure token device is carried out.

Consequently, it can only be concluded from what is actually disclosed in DiGiorgio that the challenge response authentication is carried out first of all via communication from the ISP to the local computer system 14 using, for example, a Hyper Text Transfer Protocol (see col. 7, lines 44-49) via a communications link 15, and then the computer system 14 communicates with the secure token device 10 using the Opencard standard and a Java applet API to communicate with the ISP applet 44 in the secure token device 10, as clearly disclosed at column 5, lines 26-37, and column 7, line 19, through column 9, line 43.

With respect to independent claims 1 and 42, the Office Action's proposal that "when a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33)" and "once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10 lines 33-35)" is incorrect in view of the above comments, and DiGiorgio does not disclose:

> *"a first client data processing section receiving incoming message packets from said remote computer system using said client communications section, separating encapsulated APDUs from said incoming message packets thus generating desencapsulated APDUs and routing said desencapsulated APDUs to*

said PSD through said PSD interface independently of the origin and integrity of said incoming message; and

a second client data processing section receiving incoming APDUs from said PSD interface, encapsulating said incoming APDUs into outgoing message packets and routing said outgoing message packets to said remote computer system through said client communications section."

Furthermore, DiGiorgio's user does not attempt to access services of the ISP from the token device; this is done by double clicking an icon on the local computer system 14 (see col. 10, lines 24-28).

With respect to independent method claims 20 and 29, the Office Action proposes that "when a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (col. 2 lines 16-23 & col. 10 lines 24-33)" and "once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10 lines 33-35)" is incorrect in view of the above remarks, and DiGiorgio does not disclose:

"converting on said remote computer system said request from said nonnative protocol into an APDU format request message using a first server data processing section,

encapsulating on said remote computer system said APDU format request message into said packet based communications protocol producing an encapsulated request message, using a second server data processing section, …

receiving by said client said encapsulated request message sent over said network, processing said encapsulated request message using a first data processing section to separate said APDU format request message from said encapsulated request message, …

receiving by said client said APDU format response message through said PSD Interface and encapsulating said APDU format response message into said packet based communications protocol producing an encapsulated response message, using a second data processing section,

transmitting said encapsulated response message over said network using said packet based communications protocol,

receiving said encapsulated response message sent over said network by said remote computer system, processing said encapsulated response message using a third server data processing section to separate said APDU response message from said encapsulated response message thus generating a desencapsulated APDU response message, and

converting by said remote computer system said desencapsulated APDU response message into a response in a non-native protocol using a fourth server data processing· section and forwarding said response to at least one API Level Program."

Moreover, the claimed step of "generating a request to access said PSD on said remote computer system, wherein said request is in a non-native protocol for communicating with said PSD and said request is generated by an API Level Program" is not suggested by DiGiorgio's disclosure of “a secure token device access system wherein a secure token device and a local computer system· communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 - col. 2 line 13 & Col. 9 lines 1-6)” (see Office Action page 9), as in the current invention the above request is generated at a remote computer system and in DiGiorgio it can only happen at the local computer system locally connected to the reader, as pointed out by the Office Action.

The same arguments equally apply to the subject matter of independent claim 29, as it contains similar subject matter to that of claim 20 with the additional feature that the APDU format message is encrypted using a cryptography data processing section.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,

/James Edward Ledbetter/

James E. Ledbetter
Registration No. 28,732

Date: May 1, 2008
JEL/DWW/att

Attorney Docket No. 00741-01101
Dickinson Wright PLLC
1901 L Street, NW, Suite 800
Washington, DC 20036
Telephone: (202) 659-6960
Facsimile: (202) 659-1559